UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE UNITED STATES OF AMERICA -against- KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, Defendants.	Case No.: 24-CR-82 (RMB)

AMENDED MEMORANDUM OF LAW IN SUPPORT
OF DEFENDANTS' MOTION TO DISMISS INDICTMENT

Roger A. Burlingame
Matthew L. Mazur
DECHERT LLP
Three Bryant Park
1095 Avenue of the Americas
New York, NY 10036
(212) 698-3500
roger.burlingame@dechert.com
matthew.mazur@dechert.com

Counsel for Defendant
William Lonergan Hill

Michael Kim Krouse
William T. Sharon
Maya Kouassi
ARNOLD & PORTER
KAYE SCHOLER LLP
250 West 55th Street
New York, NY 10019-9710
(212) 836-8000
michael.krouse@arnoldporter.com

Anthony J. Franze (*pro hac vice*)
ARNOLD & PORTER
KAYE SCHOLER LLP
601 Massachusetts Avenue, NW
Washington, DC 20004
(202) 942-6479
anthony.franze@arnoldporter.com

Counsel for Defendant
Keonne Rodriguez

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases **Pages:**

Statutes, Rules, & Regulations

Other Authorities

INTRODUCTION

The indictment against Defendants Keonne Rodriguez and William Lonergan Hill alleges conduct that is lawful under the relevant statutes and the government's own longstanding interpretation of those statutes. The Court should therefore dismiss both counts as a matter of law.

The indictment centers on a software application for Bitcoin users called Samourai Wallet. The government alleges that Samourai was a "cryptocurrency mixing service" and an "unlicensed money transmitting business" designed as a haven for money launderers. But far from the money-laundering bogeyman portrayed by DOJ, Samourai was designed and used—by tens of thousands of everyday people—for a legitimate purpose: to keep private financial information private.

Cryptocurrency poses unique privacy concerns. Unlike traditional credit card, ATM, checking, or other financial transactions—which are recorded on customers' *private* bank statements or financial institutions' *private* ledgers—every single cryptocurrency transaction is recorded on a *public* ledger called the "blockchain." The blockchain can be viewed by anyone with an internet connection. As a result, criminals scour the blockchain to identify accounts with substantial assets, then target account holders for fraud, scams, hacking, and even violent crime. To protect themselves, "[l]aw abiding cryptocurrency users employ mixers to maintain anonymity concerning their net worth, spending habits, and donations to political causes" and "to thwart criminals that would use this information to identify potential victims or set up phishing schemes." *Van Loon v. Dep't of the Treasury*, 122 F.4th 549, 559 (5th Cir. 2024).

Samourai Wallet and similar apps known as "CoinJoins" provided a solution to the privacy problem. Samourai operated openly in the market from 2015 through 2024, available on the Google Play Store. Its app empowered Bitcoin users to pool their transactions, making it more difficult to identify users' individual transactions and identities on the public blockchain. Essentially, Samourai allowed users to avoid posting the cryptocurrency-equivalent of their private

credit card or bank statements on the internet for all the world to see.

Critically, Samourai—unlike traditional "mixers"—was specifically designed not to be a "money transmitter" under U.S. law. As the indictment alleges, Samourai never took custody of a user's Bitcoin. Instead, the app empowered users to transact with one another, without ever surrendering their "private keys" to Samourai. Indictment ¶ 9. Because Samourai did not "transfer," "accept" or "transmit" any funds, it was simply not a money transmitting business that was required to be licensed by the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") or to implement anti-money laundering controls under the Bank Secrecy Act. Indeed, under the plain text of the statutes and FinCEN's guidance, everyone from prominent industry lawyers,[1] to cryptocurrency experts,[2] to major industry participants,[3] to members of Congress,[4] understood that selling anonymizing software did not make Samourai a money transmitting business.

---

[1] *E.g.*, Covington & Burling, *FinCEN Issues Guidance to Synthesize Regulatory Framework for Virtual Currency* (2019) ("[O]wners of unhosted wallets—computer software that allows owners to store and conduct [cryptocurrency] transactions—are not money transmitters"); King & Spalding LLP, *Tying It All Together: FinCEN Consolidates Several Years of Cryptocurrency Guidance* (2019) (similar); Morgan Lewis LLP, *FinCEN Issues Guidance on Crypto* (2019) (similar); KelmanPLLC, *Navigating FinCEN's Latest Guidance* (2024) (similar).

[2] *E.g.*, Katherine Ross & Michael McSweeny, *The DOJ's About-Face on Money Transmitters*, Blockworks (2024) ("Under clear and long established FinCEN guidance and under any common sense reading of the underlying law," noncustodial wallets "are not money transmitters" (quoting cryptocurrency expert)); Peter Van Valkenburgh, *DOJ's New Stance on Crypto Wallets is a Threat to Liberty and the Rule of Law*, Coin Center (2024) ("It has been the clear and consistent policy of the U.S. government since at least 2013 that cryptocurrency wallet developers and the users of those wallets are not money transmitters"); Seth for Privacy, *How Samourai Wallet Worked and Why It Matters*, FreedomTech (2024) (similar).

[3] *E.g.*, Letter to Senate Committee on Banking et al. from Industry Participants (2025) ("The DOJ's new policy position, first debuted in August 2023 via criminal indictment, creates confusion and ambiguity with the spectre of criminal liability, and ultimately threatens the viability of U.S.-based software development in the digital asset industry and other industries.").

[4] Letter from Senators Lummis and Wyden to U.S. Attorney General Merrick Garland (2024) ("Consistent with Congress' intent, statutory language and existing regulations, FinCEN has consistently taken this same position in published guidance that non-custodial services are not within the scope of money transmission registration requirements.").

Nevertheless, in an apparent power struggle with FinCEN, DOJ departed from the settled interpretation of "money transmitting business" and alleged that Samourai Wallet *was* a money transmitter. The DOJ charged Defendants with (1) conspiring to operate "an unlicensed money transmitting business" in violation of 18 U.S.C. § 1960; and (2) conspiring with unidentified Samourai users to commit money laundering in violation of 18 U.S.C. § 1956. The indictment is legally defective and should be dismissed under Federal Rule of Criminal Procedure 12(b)(3).

First, Defendants did not operate a "money transmitting business," a threshold requirement under Section 1960. The indictment itself alleges that Samourai users never surrendered custody or control over their cryptocurrency by providing their "private keys." Indictment ¶ 13. Thus, Samourai did not "transfer," "accept," or "transmit" any currency, which is the *sine qua non* of a money transmitter. The indictment also asserts that Samourai was privacy "software," *id.*, but ignores FinCEN's longstanding guidance that "suppliers of . . . anonymizing software" are not money transmitters.

Second, Defendants did not conspire with users of Samourai Wallet to commit money laundering under Section 1956. For one, the indictment alleges that Defendants violated Section 1956 by using a "financial institution" to conceal or disguise proceeds of specified unlawful activity. *Id.* ¶ 30. But Samourai Wallet was an app, not a "financial institution" as defined by the statute. 18 U.S.C. §§ 1956(a)(1)(B)(i), (c)(4)(B).

For another, DOJ's theory—that a person or business "conspires" with app users simply by allegedly knowing that some segment of their customers will misuse their product—contravenes longstanding Supreme Court precedent and common sense. It's akin to charging an encrypted messaging app developer with conspiracy because it may know that some customers use the app to communicate about financial crimes. Or charging a burner phone manufacturer because it may

know some customers use the phones to facilitate drug crimes. Or charging a shovel manufacturer because it may know murderers use shovels to bury victims—etcetera, etcetera, etcetera. Such knowledge does not make out a conspiracy among the buyers and the sellers.

If the government wants to adopt a new policy requiring non-custodial anonymizing software providers to obtain licenses and implement anti-money laundering controls, the proper course is the legislative and rulemaking process, not criminal charges. Indeed, both Republican and Democratic U.S. Senators have decried *this prosecution* as an "unprecedented interpretation of" the applicable statutes and regulations that "contradicts the clear intent of Congress and the authoritative guidance of [FinCEN]." *Supra* n.4. Industry participants have also lamented the chilling effect of the prosecution on software developers.[5] Members of Congress have recently proposed bills,[6] and FinCEN is engaged in notice-and-comment rulemaking, concerning regulation of anonymizing apps.[7] This prosecution is an improper end run around these procedures and due process, which guarantees fair notice of what acts constitute crimes. The Court should dismiss the indictment as a matter of law.

LEGAL STANDARD

Under Federal Rule of Criminal Procedure 12(b)(3), a court may dismiss based on a "defect in the indictment," which includes "failure to state an offense." "Since federal crimes are 'solely creatures of statute,' a federal indictment can be challenged on the ground that it fails to allege a crime within the terms of the applicable statute." *United States v. Aleynikov*, 676 F.3d 71, 75-76 (2d Cir. 2012). Though indictments are dismissed sparingly, courts do not hesitate to dismiss where

[5] Letter to the Senate Committee on Banking et al. from Industry Participants (2025).

[6] *See* Nicholas Anthony, *The Blockchain Integrity Act: Latest Attempt to Restrict Financial Privacy*, Cato Institute (2024); H. R. 3533, 119st Cong. (2025).

[7] *See* Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72701 (2024).

the charges stem from an erroneous interpretation of a criminal statute. *See id.* (affirming dismissal of indictment based on legally incorrect interpretation of terms "goods," "wares," or "merchandise" under National Stolen Property Act); *United States v. Pirro*, 212 F.3d 86, 92-93 (2d Cir. 2000) (affirming dismissal of indictment based on legally incorrect interpretation of terms in criminal tax statutes); *United States v. Heicklen*, 858 F. Supp. 2d 256, 275-76 (S.D.N.Y. 2012) (dismissing indictment based on prosecution's legally incorrect interpretation of "issue or matter" in statute prohibiting attempts to influence jurors). That is the proper course here.

BACKGROUND

A. Cryptocurrency, Privacy, and CoinJoin Apps

Cryptocurrency is a digital system of money used by tens of millions of Americans. Scott Reeves, *46 Million Americans Now Own Bitcoin, as Crypto Goes Mainstream*, Newsweek (2021). Thousands of American businesses now accept cryptocurrency as a form of payment. Tim Davis et al., *The Use of Cryptocurrency in Business*, Deloitte, 3 (2023). Bitcoin is a type of cryptocurrency. *United States v. Harmon*, 474 F. Supp. 3d 76, 80 (D.D.C. 2020). "Transferring or otherwise using a bitcoin requires an address, a public encryption key, and a private encryption key." *Id.* "To transfer bitcoin from one address to another, the sender transmits a message—called a transaction—on the Bitcoin public network." *Id.* (citing Jerry Brito et al., *The Law of Bitcoin* 31 (Stuart Hoegner ed., 2015)). "The transaction must contain: (1) the amount of bitcoin to be transferred; (2) the address to which the bitcoin will be sent; (3) the address from which the bitcoin is being sent; and (4) the public key associated with the sender and the sending address." *Id.* (citing Shawn Amuial, *The Blockchain: A Guide for Legal & Business Professionals* § 1:3 (2016)). "With these elements in place, the sender must sign the transaction using a digital signature generated using the sender's private key." *Id.*

One unique feature of Bitcoin is that it operates on an open and decentralized blockchain. The blockchain is like a bank's ledger in that it records all transactions. *Harmon*, 474 F. Supp. 3d 76, 80. But unlike a bank's ledger, the blockchain is public. Users must disclose their Bitcoin addresses when they conduct transactions. And "[i]f someone obtains information that allows them to link a blockchain address to an entity, they may effectively observe that entity's entire transaction history and associated activity." Matthias Nadler & Fabian Schar, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, Fed. Reserv. Bank of St. Louis (2023); *accord* Hugo Schnoering & Michalis Vazirgiannis, *Heuristics for Detecting CoinJoin Transactions on the Bitcoin Blockchain*, ResearchGate (2023).

Indeed, an entire industry has arisen to do just that. Companies analyze blockchain transactions to identify the people behind them. And events such as data breaches connect personally identifiable information to a Bitcoin address, allowing wrongdoers to search the blockchain and target cryptocurrency users for financial and even violent crime.[8] Physical attacks on cryptocurrency users have been rampant. *See* Maia Coleman & Chelsia Rose Marcius, *Crypto Investor Charged with Kidnapping and Torturing Man for Weeks*, N.Y. Times (2025), https://bit.ly/3TbtgVs.[9] And donors to politically-charged causes can be identified and face

[8] Rob Price, *Kidnapped for Crypto: Criminals See Flashy Crypto Owners as Easy Targets, and it has Led to a Disturbing String of Violent Robberies*, Bus. Insider (2022); Nathaniel Popper, *Bitcoin Thieves Threaten Real Violence for Virtual Currencies*, N.Y. Times (2018); Andrew Chow, *A New U.S. Crackdown Has Crypto Users Worried About Their Privacy*, Time (2022).

[9] For a sample of the many reported physical attacks, *see* Known Physical Bitcoin Attacks, https://bit.ly/4kP0R3r.

retaliation.[10] The blockchain also presents baseline privacy concerns for ordinary citizens.[11] After all, no one would want their lifetime of bank transactions available for the world to see, when often those transactions reveal highly personal information. *E.g.*, Leigh Cuen, *Sexual Assault Survivor Uses Crypto to Crowdfund Anonymously*, CoinDesk (2021).

That's where software like Samourai Wallet comes in. While the government labels Samourai a mixer, the software's privacy tools are actually known as "CoinJoins"—"a commonly used method to bolster privacy for Bitcoin users. It involves a collaboration wherein individuals combine their transaction[s] into one large transaction. Consequently, tracking individual transfers becomes intricate." Schnoering et al., *supra* at 2. These apps function without a central custodian, meaning users retain control over their funds throughout the process, using their private keys. *See id.*; Bradley Rettler, *How Bitcoin CoinJoins Help Facilitate Pro-Democracy Protests*, Forbes (2024) ("In a CoinJoin, users jointly construct transactions where their coins are combined and then sent out to various addresses . . . . Since it is an automatic protocol, no coordinating authority has custody of the bitcoin involved; each user retains control of their own coins throughout.").

B. The Samourai Wallet CoinJoin App

"Many [Bitcoin] users . . . store their private keys securely in a digital wallet, which can take the form of software or hardware." *Harmon*, 474 F. Supp. 3d at 82 (citations omitted). As set forth in the indictment,[12] Samourai was a Bitcoin wallet that included privacy features allowing

[10] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure* (2022); Brad Bourque, *The Crypto Wars and the Future of Financial Privacy*, Fordham J. of Corp. & Fin. L. (2023).

[11] *See* Geoff Goodell & Tomaso Aste, *Can Cryptocurrencies Preserve Privacy and Comply with Regulations*, Frontiers in Blockchain (2019); Gary Weinstein, *AI and Blockchain Analytics: The Urgent Need for Crypto Privacy Tool*, Forbes (2023).

[12] While aspects of the indictment's description of Samourai Wallet are inaccurate, this motion assumes, as required, that the allegations in the indictment are true. *E.g.*, *Heicklen*, 858 F. Supp. 2d at 261 ("In considering a motion to dismiss, the Court relies on the indictment and accepts the allegations of the indictment as true.").

users to construct CoinJoin and intermediate "hop" transactions.

"After users download Samourai, they can store their private key for any BTC [*i.e.*, Bitcoin] address they control inside of the Samourai program." Indictment ¶ 9. The indictment acknowledges that "these private keys are not shared with Samourai employees." *Id.* The indictment focuses on two features of Samourai. First, "a cryptocurrency mixing service known as 'Whirlpool,' which coordinates batches of cryptocurrency exchanges between groups of Samourai users to prevent tracing" of transactions over the blockchain. *Id.* ¶ 10. Second, "a service called 'Ricochet,' which allows a Samourai user to build in additional and unnecessary intermediate transactions (known as 'hops') when sending cryptocurrency from one address to another address." *Id.*

Whirlpool. Whirlpool was introduced around April 2019. *Id.* ¶ 12. It allowed "user[s] [to] select[] an amount of BTC that they wish to mix and the pool in which they would like to mix that BTC." *Id.* "For example, if a user wishes to contribute 1 BTC into the 0.05 pool, the Samourai software on the user's cellphone will broadcast a transaction to the blockchain transferring 1 BTC into 19 [other] addresses, each containing approximately 0.05 BTC." *Id.* ¶ 13. "Each of these 19 addresses containing approximately 0.05 BTC will serve as an input in a Whirlpool transaction." *Id.* Then, "the Samourai application on a user's cellphone communicates to other Samourai users, and Samourai's coordinator server randomly selects four other inputs already in the selected pool [from other users], to be mixed with the new incoming input and communicates that information to each user. The [app] then broadcasts a transaction to the Blockchain in which all five inputs (each a separate address) are then transferred to five outputs (each a separate address)." *Id.*

"[A]lthough the private keys for these cryptocurrency addresses are stored in each user's individual cellphone," the indictment states, the private keys are "not shared with Samourai's

employees." *Id.* According to the indictment, "Samourai Wallet's role in this process is to 'pool' liquidity, making it easier to find other peers who want to mix the same size inputs, assist in communication between peers, and broadcasting the final signed transaction." *Id.*

Ricochet. While Ricochet's software operated differently from Whirlpool's CoinJoin feature, it also helped users keep their transactions private on the blockchain. The indictment contends that the Ricochet "hop" feature was introduced in or around 2017, allowing "a Samurai user [to] select[] an amount of [Bitcoin] that they wish to send, and the destination address where it is to be sent." *Id.* ¶ 15. With Ricochet—like Whirlpool—"the private keys for these addresses are stored in each user's individual cellphone and not shared with Samourai's employees." *Id.* Thus, like Whirlpool, Ricochet did not transfer, accept, or transmit any Bitcoin. Rather, users controlled and transmitted their own funds. Ricochet simply added stops along the public transaction history between the sender and the recipient, thus protecting the original sender's identity. "Just like Whirlpool," Ricochet "never allowed Samourai Wallet to take custody of funds or alter the flow of funds at any point." *How Samourai Wallet Worked*, *supra* n.2.

ARGUMENT

I. THE SECTION 1960 COUNT FAILS AS A MATTER OF LAW

The indictment charges Defendants with conspiracy to operate an "unlicensed money transmitting business" under 18 U.S.C. § 1960(b). The indictment initially identified two purported objects of the conspiracy to violate: (1) Section 1960(b)(1)(B), which defines "unlicensed money transmitting business" as one that "fails to comply with the money transmitting business registration requirements under [the Bank Secrecy Act (31 U.S.C. § 5330) and its implementing] regulations"; and (2) Section 1960(b)(1)(C), which defines "unlicensed money transmitting business" as one that "otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense

or are intended to be used to promote or support unlawful activity." *See* Indictment ¶¶ 1, 31-34. The DOJ has since advised that it will not proceed under Section (b)(1)(B).

Regardless, "to have violated either § 1960(b)(1)(B) or § 1960(b)(1)(C), [a defendant] had to have been considered a 'money transmitting business.'" *United States v. Pilipis*, 2025 WL 486604, at *4 (S.D. Ind. Feb. 13, 2025). Thus, the threshold question before considering any violation of Section (b)(1)(B) or (b)(1)(C) is whether Samourai Wallet was a "money transmitting business." If not, the 1960 count must be dismissed.

A. Samourai Wallet Was Not a "Money Transmitting Business"

Section 1960 defines "money transmitting" as "*transferring* funds on behalf of the public by any and all means including but not limited to *transfers* . . . by wire, check, draft, facsimile, or courier." *Id.* § 1960(b)(2) (emphases added). A money transmitting business, then, is a business engaged in "transferring funds on behalf of" someone to someone else. Though the statute does not define "transferring," the ordinary meaning of "transfer" is "to convey from one person, place, or situation to another." *Transfer*, Merriam-Webster, https://bit.ly/4mJknA3; *accord Transfer*, Oxford English Dictionary (3d ed. 2002) (similar).

Applying that ordinary meaning, the Second Circuit has held that a money transmitting business is one that "*receives* money from a customer and then, for a fee paid by the customer, *transmits* that money to a recipient." *United States v. Velastegui*, 199 F.3d 590, 592 (2d Cir. 1999) (emphases added). And other courts have thus repeatedly held that money transmission requires the "movement of funds" by the defendant. *United States v. $1,370,851 in U.S. Currency*, 2010 WL 11650916, at *5 (S.D. Fla. Oct. 6, 2010) (Section 1960 requires that defendant "transmitted money received or belonging to others"); *Givelify LLC v. Dep't of Banking and Sec.*, 210 A.3d 393, 401-02 (Pa. Commw. Ct. 2019) (software provider did not "transmit" money because funds were "never deposited into an account directly owned or controlled by petitioner"); *Harmon*, 474 F.

Supp. 3d at 103 (Section 1960 "seemingly require[s] a money transmitting business to move funds from one person or place to another."); Barabander, *supra* at 16 n.47 (surveying caselaw and "not identify[ing] a single . . . case where a party was 'money transmitting' under Section 1960 and did not obtain and relinquish control over funds").

Here, the indictment does not allege that Samourai Wallet or Defendants transferred Bitcoin on behalf of someone to someone else. As the indictment alleges, "the Samourai application on a user's cellphone communicates with other Samourai users" to help *users* pool transactions to make them less visible on the blockchain. Indictment ¶ 13. Critically, "the private keys for the[] cryptocurrency addresses" to which *users* transmitted funds were "stored in each user's individual cellphone and not shared with Samourai's employees." *Id.* Samourai was a non-custodial coordinating server, meaning *users*—not Samourai or its providers—transmitted their own cryptocurrency and simply used the app to maintain the privacy of their financial transactions.

As members of Congress recognized in criticizing this indictment: "The DOJ's unprecedented interpretation of this statute in the context of non-custodial crypto asset software services contradicts the clear intent of Congress and the authoritative guidance of [FinCEN]. This interpretation threatens to criminalize Americans offering non-custodial crypto asset software services." Letter from Senators Lummis & Wyden to U.S. Attorney General Merrick Garland (2024). Contrary to DOJ's interpretation, "non-custodial crypto service providers cannot be classified as money transmitter businesses because users of such services retain sole possession and control of their crypto assets." *Id.* The indictment thus fails out of the gate because Samourai Wallet was not a "money transmitting business," the threshold requirement under Section 1960.

B. Samourai Wallet Was Anonymizing Software That FinCEN Advised Is Not a Money Transmitting Business

The government's longstanding view of who must register as a "money transmitter" reinforces that Samourai Wallet was not a "money transmitting business" under Section 1960. A "money transmitting business" can be liable under Section 1960 only if it (1) "fails to comply with the money transmitting business registration requirements under [31 U.S.C. § 5330], or regulations prescribed under such section," 18 U.S.C. § 1960(b)(1)(B); or (2) "otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity." *id.* § 1960(b)(1)(C).

The text and FinCEN's guidance underscore that Samourai Wallet was not a "money transmitting business." Section 5330 defines a "money transmitting business" as any business that provides "money transmitting . . . services, or issues or redeems money orders, travelers' checks, and other similar instruments or any other person who engages as a business in the transmission of currency." 31 U.S.C. § 5330(d)(1)(A). The statute defines "money transmitting service[s]," in turn, as "*accepting* currency, funds, or value that substitutes for currency and *transmitting* the currency, funds, or value that substitutes for currency by any means." *Id.* § 5330(d)(2). To "accept" means to "receive (something offered) willingly" or to "take or receive (something offered)." *Accept*, Merriam-Webster, https://bit.ly/3FME0Xl. To "transmit" means "to send or convey from one person or place to another." *Transmit*, Merriam-Webster, https://bit.ly/4mLvBnP. Just as Samourai Wallet did not "transfer" funds, *see supra* I.A., it did not "accept" or "transmit" currency.

Indeed, Samourai Wallet was precisely the type of business that FinCEN has long advised the industry is *not* a money transmitting business. In 2014, FinCEN published an administrative ruling explaining that activities that "involve neither 'acceptance' nor 'transmission' of the

convertible virtual currency . . . are not the transmission of funds within the meaning of the Rule." FinCEN, *Application of FinCEN Regulations to Virtual Currency Mining Operations* 3 (Jan. 30, 2014). In 2019, FinCEN published a detailed guidance "to remind persons . . . how FinCEN regulations . . . apply to certain business models involving [cryptocurrency]." FinCEN Guidance, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, 1 (May 9, 2019) ("FinCEN 2019 Guidance") (footnote omitted). The guidance reiterated that "money transmission services . . . mean *the acceptance of* currency . . . from one person *and the transmission of* currency . . . to another location or person by any means." *Id.* § 1.2.1. A "money transmitter" is one whose "activities include *receiving* one form of value [including cryptocurrency] from one person and *transmitting* either the same or a different form of value to another person or location, by any means." *Id.* § 2 (emphases added).

In a section concerning the "Transmission of [cryptocurrency]," FinCEN observed that "a person still qualifies as a money transmitter if that person's activities include *receiving* [cryptocurrency] from one person and *transmitting* [it] to another person or location." *Id.* (emphases added). Critically, FinCEN emphasized that an "anonymizing software provider is not a money transmitter." *Id.* § 4.5.1(b). It distinguished "anonymizing *services* providers"—sometimes called "mixers"—from "anonymizing *software* provider[s]." *Id.* § 4.5.1. An anonymizing *service* provider "accept[s cryptocurrencies] and retransmit[s] them in a manner designed to prevent others from tracing the transmission back to [the] source." *Id.* § 4.5.1. These are money transmitting businesses because they "accept[] value from a customer and transmit[] the same or another type of value to the recipient." *Id.* § 4.5.1(a).

By contrast, "FinCEN regulations exempt from the definition of money transmitter those persons providing 'the delivery, communication, or network access services used by a money

transmitter to support money transmission services.'" *Id.* § 4.5.1(b) (quoting 31 C.F.R. § 1010.100(ff)(5)(ii)). "This is because suppliers of tools (communications, hardware, or software) that may be utilized in money transmission, *like anonymizing software*, are engaged in trade and not money transmission." *Id.* (emphasis added). Thus, an "anonymizing software provider" like Samourai "is not a money transmitter." *Id.*; Benjamin Gruenstein et. al., *Secret Notes and Anon. Coins: Examining FinCEN's 2019 Guidance on Money Transmitters in the Context of the Tornado Cash Indictment,* Int'l Acad. of Fin. Crime Litigators 8 (Sept. 2023) ("[T]o act as a money transmitter, a party must have necessary and sufficient control over the value being transmitted.").

C. The Government's Change of Position Deprived Defendants of Fair Notice

"A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012); *Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 156 & n.15 (2012) ("[A]gencies should provide regulated parties 'fair warning of the conduct [a regulation] prohibits or requires'"). "This requirement of clarity in regulation is essential to the protections provided by the Due Process Clause of the Fifth Amendment." *Fox*, 567 U.S. at 253. A conviction "fails to comply with due process if the statute or regulation under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *Id.*

In *Fox*, for instance, the FCC in 2001 had issued guidance that a key consideration on whether a television broadcast was "actionably indecent" was "whether the material dwelled on or repeated at length the offending description or depiction." *Id.* at 254. Three years later, "the Commission changed course and held that fleeting expletives could be a statutory violation." *Id.* The FCC charged broadcasters with violating the "fleeting expletives" standard even though the broadcasts had occurred before 2003. *Id.* The Supreme Court held this violated due process

because the "lack of notice to Fox and ABC that [the] interpretation had changed so the fleeting moments of indecency contained in their broadcasts were a violation of [the governing statute] as interpreted and enforced by the agency fail[ed] to provide a person of ordinary intelligence fair notice of what is prohibited." *Id.* (citations omitted); *see United States v. Harra*, 985 F.3d 196, 212-13 (3d Cir. 2021) ("[D]ue process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." (collecting cases)).

The prosecution here similarly violates Defendants' due process rights. During the decade Samourai Wallet operated, courts held that money transmission involves the transfer of funds. And the government, through FinCEN, advised that companies and software apps that did not "accept" or "transmit" funds were not "money transmitting" businesses. *See supra* I.B. The FinCEN 2019 Guidance could not have been clearer when it confirmed that custodial "mixers" (services that accepted and transmitted funds from users) were money transmitting businesses, while noncustodial anonymizing software providers ("suppliers of software a [cryptocurrency owner] would use for the same purpose") were not. FinCEN 2019 Guidance § 4.5.1. To change course now would deprive Defendants' of fair notice, since Samourai Wallet was—as the indictment alleges—"software" employed by users to anonymize their transactions.

Indeed, the DOJ has recently observed through the so-called "Blanche Memo" that "the prior Administration used the Justice Department to pursue a reckless strategy of regulation by prosecution, which was ill conceived and poorly executed." Memorandum from the Deputy Attorney General on Ending Regulation by Prosecution (Apr. 7, 2025). The Blanche Memo notes that DOJ will "no longer target virtual currency exchanges, mixing and tumbling services, and offline wallets for the acts of their end users." The Blanche Memo reflects that industry participants

like Defendants were caught in the crossfire between DOJ's aggressive new regulatory position and FinCEN's longstanding approach to anonymizing software like Samourai Wallet. DOJ's "reckless strategy of regulation by prosecution" deprived Defendants of fair notice. *Id.*

If there were any doubt, the Court should construe Sections 1960 in Defendants' favor under established canons of construction. One, the doctrine of constitutional avoidance demands that the Court interpret the statute in a way that avoids doubts about its constitutionality. *Nielsen v. Preap*, 586 U.S. 392, 418-19 (2019). The only way to avoid doubts about the constitutionality of the laws here is to reject DOJ's newfound interpretation, which would deprive Defendants and other software developers of fair notice as to the conduct that was prohibited.

Two, where "the government has repeatedly issued guidance to the public at odds with the interpretation it now asks [the court] to adopt," there is reason "to question whether its current position represents the best view of the law." *Bittner v. United States*, 598 U.S. 85, 97 (2023). And where the relevant federal regulator has consistently interpreted a statute to mean one thing, "there can be no doubt that traditional notions of fairness inherent in our system of criminal justice prevent the Government from proceeding with [a] prosecution" based on a *different* interpretation. *United States v. Penn. Indus. Chem. Corp.*, 411 U.S. 655, 674 (1973). That is the case here.

Three, under the rule of lenity, "when [a] choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before [courts] choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *Aleynikov*, 676 F.3d at 82. Here, that would mean choosing the interpretation that non-custodial apps like Samourai Wallet are not "money transmitting businesses."

D. Judge Failla's Bench Order in *Tornado Cash* Is Inapposite

In *Tornado Cash*, DOJ similarly urged an unprecedented interpretation of "money

transmitting business."[13] In September 2024, Judge Failla issued an unwritten order from the bench that "somewhat summarily" denied the defendant's motion to dismiss.[14] While that decision is not binding in this Court,[15] it is inapposite anyway.

First, Judge Failla found that the defendant proffered "factual arguments," which are not permissible on a motion to dismiss. Tr. at 18-20. Here, the challenge is to the face of the indictment and takes all of its allegations as true—including the description of Samourai Wallet. *See supra* n.12. Further, *Tornado Cash* did not involve a CoinJoin, but fundamentally different applications.

Second, Judge Failla found that the Section 1960 claim against the defendant there should not be dismissed for various reasons that do not bear on this case. The court concluded that it was "required to accept at this stage the allegations of the indictment that the charged money transmitting business included conduct of Tornado Cash's founders and network of relayers, and not merely the pool." Tr. at 21. But the indictment here alleges that Samourai Wallet was software that *users*, not Defendants, employed to transmit funds. Indictment ¶ 13.

Third, Judge Failla appeared to find that the Bank Secrecy Act, 31 U.S.C. § 5330(d)(1)(A) defines money transmission business not just as the transmission and acceptance of funds, but also as *facilitating* transmission. But that overlooks key features of the statutory provisions.

Before a court considers whether an entity complied with the BSA, it must first determine that the entity is a "money transmitting business" under Section 1960, which does not criminalize

---

[13] Unsealed Indictment, *United States v. Storm*, No. 23-CR-430 (KPF) (S.D.N.Y. Aug. 21, 2023), ECF No. 1.

[14] *See* Transcript of Sept. 25, 2024 Conference ("Tr.") at 17, *United States v. Storm*, No. 23-CR-430 (KPF) (S.D.N.Y. Oct. 3, 2024), ECF No. 84.

[15] *Preble-Rish Haiti, S.A. v. Republic of Haiti*, 2023 WL 4210057, at *1 (S.D.N.Y. June 27, 2023) ("A decision of a federal district court judge is not binding precedent in either a different judicial district, the same judicial district, or even upon the same judge in a different case." (citations omitted)).

facilitating transactions. Rather, it defines money transmitting as "transferring funds on behalf of the public by any and all means including but not limited to transfers . . . by wire, check, draft, facsimile, or courier." 18 U.S.C. § 1960(b)(2). If Congress had wanted to define a money transmitting business as one that merely facilitates someone else's transfer of funds, it would have.

Further, Judge Failla misinterpreted the Bank Secrecy Act. Judge Failla referenced Section 5330(d)(1)(A), which defines a money transmission business as "any person who engages as a business in an informal money transfer system or any network of people who engage as a business in *facilitating* the transfer of money domestically or internationally outside of the conventional financial institutions system." Tr. at 22 (emphasis added). But the remaining part of that provision clarifies that it applies only to "a business in the *transmission* of currency, . . . *including* . . . any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system." "Transmission of currency" is still necessary, 31 U.S.C. § 5330(d)(1)(A), and is absent here.

Finally, Judge Failla acknowledged that although the FinCEN 2019 Guidance "does speak of control" of the cryptocurrency as a prerequisite to being a money transmitter, Section 1960 "[a]t its core . . . seeks to prevent the unlicensed transmission of customer funds from one location to another, irrespective of whether the transmitter obtained temporary control over the funds to effectuate the transfer or constructed the transfers specifically in a matter to avoid such control." Tr. at 22. Judge Failla concluded that, regardless whether the software took custody of the cryptocurrency, it sufficed that it served the same *purpose* as "cryptocurrency mixing services recognized as money transmitting businesses." *Id.*

Putting aside that "considerations of policy divorced from the statute's text" cannot carry the day, *United States v. Tohono O'Odham Nation*, 563 U.S. 307, 317 (2011), that analysis is

irrelevant to a CoinJoin. FinCEN's guidance expressly distinguished between "anonymizing *services* providers"—so-called "mixers," where users transmit funds to a third party service that then retransmits them to help anonymize the transaction—with "anonymizing software providers," which are "suppliers of software a transmitt*or* [the cryptocurrency owner] would use for the same purpose." FinCEN 2019 Guidance § 4.5.1 (emphasis in original). An "anonymizing *software* provider is *not* a money transmitter." *Id.* § 4.5.1(b) (emphases added).

At bottom, Judge Failla made a policy determination that software that is "not meaningfully different" from custodial mixers should be treated like custodial mixers. Tr. at 22. But, as explained, Samourai was a CoinJoin, which is meaningfully different from a custodial mixer.[16]

II. THE SECTION 1956 COUNT FAILS AS A MATTER OF LAW

The indictment's remaining count asserts that Defendants conspired with unidentified users of Samourai Wallet to commit money laundering in violation of 18 U.S.C. § 1956(h). Indictment ¶¶ 29-30. The object of the conspiracy was a purported agreement to violate Section 1956(a)(1)(B)(i), called "transaction" money laundering. *Id.* To state a cognizable count under these provisions, the government must plead and prove that a defendant "agreed to: (1) conduct a financial transaction; (2) involving the proceeds of specified unlawful activity; (3) knowing that the property involved in the transaction represented the proceeds of some form of unlawful activity; and (4) knowing that the financial transaction was designed in whole or in part to conceal or disguise the nature, source, location, ownership, or control of those proceeds." *United States v. Henry*, 325 F.3d 93, 103 (2d Cir. 2003). Because a jury could not find Defendants guilty on the facts alleged and conceded in the indictment, the Section 1956 count must be dismissed.

[16] For additional problems with the *Tornado Cash* order, *see* Barabander, *supra* at 23-32.

A. Samourai Wallet Was Not a "Financial Institution"

The indictment alleges that Defendants conspired to conceal or disguise proceeds of specified unlawful activity "involv[ing] the use of a financial institution" in violation of 18 U.S.C. § 1956(a)(1)(B)(i). Indictment ¶ 30. But Samourai was not a "financial institution."

Section 1956(a)(1)(B)(i) prohibits attempting "a financial transaction" while "knowing that the property involved in [that] financial transaction represents the proceeds of some form of unlawful activity," and "knowing that the transaction is designed in whole or in part" to "conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds." 18 U.S.C. § 1956(a)(1)(B)(i). The statute defines "financial transaction" as "a transaction involving the use of a *financial institution*." 18 U.S.C. § 1956(c)(4)(B) (emphasis added). And the statute defines "financial institution" as that term is "defined in [BSA § 5312(a)(2)]." 18 U.S.C. § 1956(c)(6)(A). As relevant here, that means any business engaged "in the *transmission* of currency," 31 U.S.C. § 5312(a)(2)(R) (emphasis added)—*i.e.*, a money transmitter.

As demonstrated, however, Samourai was *not* a money transmitter. *See supra* I. Thus, Samourai was not a financial institution, so the Section 1956 claim is legally defective. *See* 31 U.S.C. § 5330(d)(1) (applying same definition to "money transmitting business"); *United States v. Ness*, 565 F.3d 73, 79 (2d Cir. 2009) (rejecting theory that defendant was a money transmitter and holding, in turn, that defendant was not a "financial institution").

B. The Indictment Does Not Allege a Legally Cognizable Conspiracy

Even if Samourai Wallet had been a "financial institution" (it was not), the conspiracy to launder money allegations still fail. "Conspiring to launder money requires that [1] two or more people agree to violate the federal money laundering statute, and [2] that the defendant knowingly engaged in the conspiracy with the specific intent to commit the offenses that are the objects of the conspiracy." *United States v. Garcia*, 587 F.3d 509, 515 (2d Cir. 2009) (quotation marks omitted).

The government must show "the defendant *agreed* on the essential nature of the plan, and that there was a conspiracy to commit a *particular offense* and not merely a vague agreement to do something wrong." *United States v. Lorenzo*, 534 F.3d 153, 159 (2d Cir. 2008) (emphases added). To prove a defendant acted "knowingly," the government must show that "the person charged with the conspiracy knew of the existence of the scheme alleged in the indictment and knowingly joined and participated in it." *Id.* This requires "more than evidence of a general cognizance of criminal activity, suspicious circumstances, or mere association with others engaged in criminal activity." *United States v. Ogando*, 547 F.3d 102, 107 (2d Cir. 2008). An agreement requires a "meeting of minds." *United States v. Rosenblatt*, 554 F.2d 36, 38 (2d Cir. 1977).

Here, the indictment acknowledges that "Samourai [was] used by customers all over the world," Indictment ¶ 9, and purportedly "enabled Samourai *users* to launder criminal proceeds," *id.* at ¶ 27 (emphasis added). But the indictment does not allege *Defendants* knew the purpose of any given transaction, much less that they knew of particular instances of misuse of the app. And it fails to identify any criminal meeting of the minds between Defendants and any customer.

1. The Indictment Fails to Allege That Defendants Had Knowledge of Any Conspiracy By Customers to Misuse Samourai Wallet

The indictment fails to allege the requisite knowledge of particular unlawful transactions. Over eighty years ago, Judge Learned Hand warned against overreach with claims of conspiracy: "[S]o many prosecutors seek to sweep within the drag-net of conspiracy all those who have been associated in any degree whatever with the main offenders. That there are opportunities of great oppression in such a doctrine is very plain, and it is only by circumscribing the scope of such all comprehensive indictments that they can be avoided." *United States v. Falcone,* 109 F.2d 579, 581 (2d Cir. 1940). That warning is salient here, given that Judge Hand was writing to reverse a conspiracy conviction based on the very theory the DOJ is now pursuing against Defendants.

In *Falcone*, suppliers of sugar and yeast sold the products to bootleggers knowing they would be used to make illicit alcohol. *Id.* The government charged them with a conspiracy to make alcohol. *Id.* Reversing the suppliers' convictions, Judge Hand rejected the theory that one who sells a product "becomes a conspirator with—or, what is in substance the same thing, an abettor of—the buyer because he knows that the buyer means to use the goods to commit a crime." *Id.* at 581.

In a landmark decision, the Supreme Court affirmed. *United States v. Falcone*, 311 U.S. 205 (1940). It held that knowledge a customer will use a product for criminal acts is insufficient to infer knowledge of the customer's conspiracy. *Id.* at 210. Although the indictment "alleged that [the suppliers] sold the materials mentioned knowing that they were to be used in illicit distilling" and "charg[ed] generally that all the defendants were parties to the conspiracy," it "did not allege specifically that any of [the suppliers] had knowledge of the conspiracy." *Id.* at 207-08; *see Direct Sales Co. v. United States*, 319 U.S. 703, 709 (1943) ("[O]ne does not become a party to a conspiracy by aiding and abetting it, through sales of supplies or otherwise, unless he knows of the conspiracy; and the inference of such knowledge cannot be drawn merely from knowledge the buyer will use the goods illegally."). As the Supreme Court recently reiterated, "an ordinary merchant does not become liable for all criminal misuses of his goods even if he knows that in some fraction of cases misuse will occur." *Smith & Wesson Brands, Inc. v. Estados Unidos Mexicanos*, No. 23–1141, slip op. at 8 (U.S. June 5, 2025).

Applying *Falcone*, courts repeatedly have dismissed indictments or reversed convictions for conspiracy where the government engaged in similar overreach. In *United States v. Superior Growers Supply, Inc.*, 982 F.2d 173 (6th Cir. 1993), for instance, the government charged a garden supply store, its owners, and employees with conspiracy to aid the illegal manufacture of marijuana. The government alleged the defendants sold gardening equipment and supplies

knowing purchasers would use the materials to cultivate the drug. *Id.* at 175. The defendants "advertise[d] their products in 'High Times' magazine and other marijuana-related publications," "[sold] or [gave] publications concerning the growing of marijuana and other marijuana-related publications to many of their customers," and "provide[d] information and advice on the growing of marijuana to various customers." *Id.* The Sixth Circuit nevertheless affirmed dismissal of the indictment as a matter of law. It held that merely providing gardening products to customers, even advertising them as tools to illegally grow marijuana, was insufficient to establish knowledge of any *specific* conspiracy. *Id.* at 178. Put simply, "there is a gulf between knowledge and conspiracy." *United States v. Blankenship*, 970 F.2d 283, 289 (7th Cir. 1992) (applying *Falcone*).

Here, the gulf is even greater. The indictment alleges only that Defendants were supposedly generally aware that some unidentified customers could use the app to hide illicit funds, and "marketed" it for such purposes on social media. Indictment ¶¶ 27-28.[17] But it does not allege Defendants knew the purpose of any individual transaction by one of Samourai's thousands of anonymous users, let alone that any particular transaction involved the proceeds of crime. *Cf. Smith & Wesson Brands*, slip op. at 10-11 (no aiding and abetting liability where complaint failed to allege "any specific criminal transaction that the defendants (allegedly) assisted" and manufacturers "treat[ed] rogue dealers just the same as they do law abiding ones—selling to everyone, and on equivalent terms"). Developing software allegedly knowing that some customers may commit a crime is materially similar to providing sugar and yeast to customers knowing they may make illegal alcohol, or selling gardening supplies to customers knowing of—and even promoting—their marijuana cultivation. Yet here, that is the basis for the purported conspiracy.

[17] The indictment completely misses the tongue-in-cheek, attention-seeking nature of social media. In any event, none of the alleged social media "marketing" in the indictment establishes the knowledge and intent necessary to join any conspiracy to commit money laundering.

2. The Indictment Fails to Allege That Defendants Had a Meeting of the Minds and Agreed to Join Any Customers' Conspiracy

Even if a defendant knows about a particular conspiracy, merely providing goods or services that aid the conspiracy is not enough to establish an *agreement* with the customers and *intent* to join the conspiracy. "It is not enough that a defendant may have wittingly aided a criminal act or that he may have intended to do so in the future; to convict a defendant of conspiracy the government must demonstrate that the defendant agreed with others that together they would accomplish the unlawful object of the conspiracy." *United States v. Alvarez*, 610 F.2d 1250, 1255 (5th Cir. 1980). And "even if a conspiracy between two parties is established, not every act of a third person that assists in the accomplishment of the objective of the conspiracy is a sufficient basis to demonstrate his concurrence in that agreement." *Id.* at 1256.

As Judge Easterbrook explained in *Blankenship*, merely "providing assistance to a criminal organization" is not "the same thing as conspiracy." 970 F.2d at 285. Rather, "there is a difference between supplying goods to a syndicate and joining it, just as there is a difference between selling goods and being an employee of the buyer." *Id.* The Seventh Circuit reasoned: "Cargill sells malt and barley to Anheuser Busch, knowing that they will be made into beer, without being part of Busch; by parallel reasoning, someone who sells sugar to a bootlegger knowing the use that will be made of that staple is not thereby a conspirator . . . ." *Id.* "'[M]ere sellers and buyers are not automatically conspirators. If it were otherwise, companies that sold cellular phones to teenage punks who have no use for them other than to set up drug deals would be in trouble, and many legitimate businesses would be required to monitor their customers' activities." *Id.*

The indictment fails for similar reasons here. Allegedly knowing or marketing the misuse of a product differs from *agreeing* with customers and *intending to join* their broader conspiracy. Providing software allegedly knowing it will be misused by some customers to mask the proceeds

of their alleged illicit activities is materially indistinguishable from selling cell phones knowing some customers may use them to facilitate illegal drug sales. *Id.* The government's interpretation here would eviscerate the "agreement" requirement, "thus eliminating a significant limiting principle" aimed at preventing boundless secondary liability. *Twitter, Inc. v. Taamneh*, 598 U.S. 471, 490 (2023). The Court should reject that overreach and dismiss.

CONCLUSION

For the reasons above, the Court should dismiss the indictment.

Dated: June 6, 2025

Respectfully submitted,

/s/ Roger A. Burlingame
Roger A. Burlingame
Matthew L. Mazur
DECHERT LLP
Three Bryant Park
1095 Avenue of the Americas
New York, NY 10036
(212) 698-3500
roger.burlingame@dechert.com
matthew.mazur@dechert.com

Counsel for Defendant
William Lonergan Hill

/s/ Michael Kim Krouse
Michael Kim Krouse
William T. Sharon
Maya Kouassi
ARNOLD & PORTER
KAYE SCHOLER LLP
250 West 55th Street
New York, NY 10019-9710
(212) 836-8000
michael.krouse@arnoldporter.com

Anthony J. Franze (*pro hac vice*)
ARNOLD & PORTER
KAYE SCHOLER LLP
601 Massachusetts Avenue, NW
Washington, DC 20004
(202) 943-6479
anthony.franze@arnoldporter.com

Counsel for Defendant
Keonne Rodriguez